AMENDMENTS TO THE CLAIMS

1. (Previously presented) A cryptographic device, comprising:

means for performing one or more cryptographic operations; and

a data storage device or devices for storing access permission data representing the availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein the data storage device or devices are adapted to enable all of the access permission data of the cryptographic device to be stored in the data storage device or devices after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed.

2. (Original) A cryptographic device as in Claim 1, wherein the data storage device is a programmable read-only memory.

3. (Original) A cryptographic device as in Claim 1, wherein the cryptographic characteristics include one or more of the following: availability of direct access to one or more mathematical primitive operations, availability of public key

encryption, permissible maximum length of public key, permissible maximum length of DES key, and availability of DES key encryption.

4. (Previously presented) A computer readable storage medium or media of a cryptographic device, the computer readable storage medium or media encoded with instructions and/or data, comprising:

instructions and/or data for performing one or more cryptographic operations; and

access permission data stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more cryptographic operations are performed by the cryptographic device, wherein all of the access permission data is stored in a storage medium or media after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the storage medium or media, the value or values of the access permission data cannot be changed.

5. (Previously presented) A computer readable storage medium or media as in Claim 4, wherein the cryptographic characteristics include one or more of the following: availability of direct access to one or more mathematical primitive operations, availability of public key encryption,

permissible maximum length of public key, permissible maximum length of DES key, and availability of DES key encryption.

6. (Previously presented) A cryptographic device, comprising:

a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;

one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

7. (Original) A cryptographic device as in Claim 6, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

8. (Original) A cryptographic device as in Claim 7, wherein the mathematical primitive operations include one or more of the following: a mod reduce operation, an add operation, a subtract operation, a multiply operation, a divide operation, an exponentiate operation, an inverse modulo operation, an XOR operation, a DES operation and an random number generator operation.

9. (Original) A cryptographic device as in Claim 6, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.

10. (Original) A cryptographic device as in Claim 6, wherein the first set of instructions and/or data used to perform one or more sub-operations are stored in a read-only memory device.

11. (Original) A cryptographic device as in Claim 10, wherein at least some of the second set of instructions and/or data used to perform the one or more cryptographic operations are stored in an erasable programmable read-only memory device.

12. (Original) A cryptographic device as in Claim 11, wherein at least some of the second set of instructions and/or data used to perform the one or more cryptographic operations are stored in a read-only memory device.

13. (Original) A cryptographic device as in Claim 6, wherein at least some of the second set of instructions and/or data used to perform the one or more cryptographic operations are stored in an erasable programmable read-only memory device.

14. (Previously presented) A computer readable storage medium or media encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:

a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation;

a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part.

15. (Previously presented) A computer readable storage medium or media as in Claim 14, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

16. (Previously presented) A computer readable storage medium or media as in Claim 15, wherein the mathematical primitive operations include one or more of the following: a mod reduce operation, an add operation, a subtract operation, a multiply operation, a divide operation, an exponentiate operation, an inverse modulo operation, an XOR operation, a DES operation and an random number generator operation.

17. (Previously presented) A computer readable storage medium or media as in Claim 14, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.

18. (Previously presented) A computer readable storage medium or media as in Claim 4, further comprising a programmable read-only memory for storing the access permission data.

19. (Previously presented) A cryptographic device as in Claim 6, further comprising means for controlling access to the first and second sets of instructions and/or data, wherein:

the means for controlling access to the first and second set of instructions and/or data comprises the means for allowing access to the first set of instructions and/or data; and

the means for allowing access to the first set of instructions and/or data does not enable access to the second set of instructions and/or data.

20. (Previously presented) A computer readable storage medium or media as in Claim 14, further comprising a fourth set of instructions and/or data for controlling access to the first and second sets of instructions and/or data, wherein:

the fourth set of instructions and/or data comprises the third set of instructions and/or data; and

the third set of instructions and/or data does not enable access to the second set of instructions and/or data.

21. (Currently amended) A cryptographic device, comprising:

a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;

one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause

performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for ~~allowing~~ enabling a third set of instructions and/or data that is distinct from both the first and second sets of instructions and/or data, ~~and~~ that is used to perform one or more cryptographic operations, and that includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed to, after manufacture of the cryptographic device, be stored on the one or more data storage devices~~, and/or cause performance of instructions and/or access of data from the first set of instructions from a device external to the cryptographic device~~.

22. (New) A cryptographic device as in Claim 21, wherein the first set of instructions and/or data used to perform one or more sub-operations are stored in a read-only memory device.

23. (New) A cryptographic device as in Claim 21, wherein at least some of the second and/or third sets of instructions and/or data used to perform one or more cryptographic operations are stored in an erasable programmable read-only memory device.

24. (New) A cryptographic device as in Claim 6, wherein the means for allowing comprises:

one or more data storage devices for storing access permission data representing the availability of access to the first set of instructions and/or data from a device external to the cryptographic device; and

a processor for executing instructions and/or accessing data to evaluate a request from a device external to the cryptographic device, in view of the access permission data, to determine whether the external device is allowed to access the first set of instructions and/or data.